PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) **Classification internationale des brevets** [7] : **H04L 9/32** — **A1**

(11) **Numéro de publication internationale:** **WO 00/45549**

(43) **Date de publication internationale:** 3 août 2000 (03.08.00)

(21) **Numéro de la demande internationale:** PCT/FR00/00174

(22) **Date de dépôt international:** 26 janvier 2000 (26.01.00)

(30) **Données relatives à la priorité:**
99/00887 27 janvier 1999 (27.01.99) FR

(71) **Déposant** *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, Place d'alleray, F–75015 Paris (FR).

(72) **Inventeurs; et**
(75) **Inventeurs/Déposants** *(US seulement)*: GIRAULT, Marc [FR/FR]; 9 Rue Bernard Vanier, F–14000 Caen (FR). PAILLES, Jean–Claude [FR/FR]; 4 Rue Des Loisirs, F–14610 Epron (FR).

(74) **Mandataire:** DU BOISBAUDRY, Dominique; Société De Protection Des Inventions, 3, Rue Du Docteur Lancereaux, F–75008 Paris (FR).

(81) **Etats désignés:** CA, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) **Title:** AUTHENTICATING OR SIGNATURE METHOD WITH REDUCED COMPUTATIONS

(54) **Titre:** PROCEDE D'AUTHENTIFICATION OU DE SIGNATURE A NOMBRE DE CALCULS REDUIT

(57) **Abstract**

The invention concerns a method wherein one first entity to be authenticated, having a public key v and a secret key s, said keys being connected by $v=s^t \pmod n$ wherein n is an integer called modulus and t a parameter, and a second authenticating entity, which knows the public key v. Said method comprises zero–knowledge data exchanges between the entity to be authenticated and the authenticating entity and cryptographic computations concerning said data, some of the computations being performed modulo n. The method is characterised in that the modulus n is particular to the authenticated entity, which communicates said modulus to the authenticating entity.

(57) **Abrégé**

Le procédé met en oeuvre une première entité "à authentifier", possédant une clé publique v et une clé secrète s, ces clés étant reliées par $v=s^{-t} \pmod n$ où n est un entier appelé module et t un paramètre, et une seconde entité "authentifiante", connaissant la clé publique v. Ce procédé comprend des échanges d'informations du type à apport nul de connaissance entre l'entité à authentifier et l'entité authentifiante et des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo n. Le procédé de l'invention est caractérisé en ce que le module n est propre à l'entité authentifiée, laquelle communique ce module à l'entité authentifiante